

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-315201

(P2000-315201A)

(43) 公開日 平成12年11月14日 (2000. 11. 14)

(51) Int.Cl.⁷

G 0 6 F 17/10

識別記号

F I

G 0 6 F 15/31

テーマコード* (参考)

Z 5 B 0 5 6

審査請求 未請求 請求項の数 8 O L (全 16 頁)

(21) 出願番号

特願平11-124804

(22) 出願日

平成11年4月30日 (1999. 4. 30)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 藤田 八郎

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 吉田 英夫

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74) 代理人 100066474

弁理士 田澤 博昭 (外 1 名)

Fターム(参考) 5B056 AA01 AA04 BB00 FF01 FF02

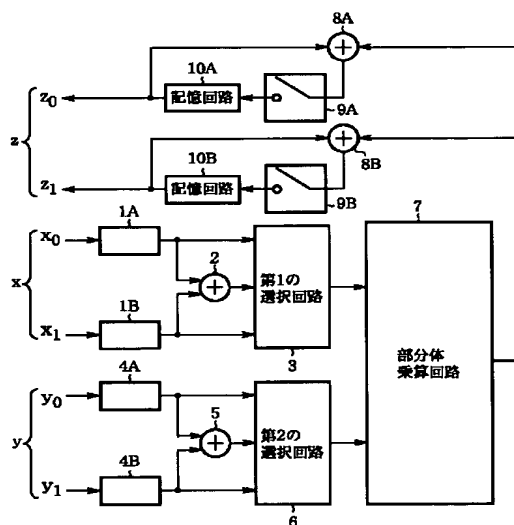
FF05

(54) 【発明の名称】 ガロア体乗算回路およびガロア体逆元演算回路

(57) 【要約】

【課題】 演算回路全体の回路規模を低減することが困難であった。

【解決手段】 第1の選択回路3は部分体元 x_0 、部分体元 x_1 および部分体元 x_0 、 x_1 の和のうちのいずれかを選択し、第2の選択回路6は部分体元 y_0 、部分体元 y_1 および部分体元 y_0 、 y_1 の和のうちのいずれかを選択し、選択された部分体元の積が部分体乗算回路7により演算される。第3および第4の部分体加算回路8A、8B並びにスイッチ回路9A、9Bはそれぞれ所定のタイミングにおいて第3および第4の部分体加算回路8A、8Bによる和で、元 x 、 y の積 z に対応する記憶回路10A、10Bに記憶された部分体の元 z_0 、 z_1 を累積更新する。



2: 第1の部分体加算回路
5: 第2の部分体加算回路
8A: 第3の部分体加算回路
8B: 第4の部分体加算回路
9A: スイッチ回路 (第1の更新回路)
9B: スイッチ回路 (第2の更新回路)
10A: 記憶回路 (第1の記憶回路)
10B: 記憶回路 (第2の記憶回路)

1

【特許請求の範囲】

【請求項 1】 ガロア体の第 1 の元と第 2 の元との積を演算するガロア体乗算回路において、

n を奇数とするガロア体 $GF(2^{2n})$ の部分体 $GF(2^n)$ の元であって前記ガロア体 $GF(2^{2n})$ の第 1 の元に対応する第 1 の部分体元および第 2 の部分体元の和を第 3 の部分体元として演算する第 1 の部分体加算回路と、

前記部分体の元であって前記ガロア体 $GF(2^{2n})$ の第 2 の元に対応する第 4 の部分体元と第 5 の部分体元との和を第 6 の部分体元として演算する第 2 の部分体加算回路と、

前記第 1 の部分体元、前記第 2 の部分体元および前記第 3 の部分体元のうちのいずれかを選択する第 1 の選択回路と、

前記第 4 の部分体元、前記第 5 の部分体元および前記第 6 の部分体元のうちのいずれかを選択する第 2 の選択回路と、

前記第 1 の選択回路により選択された部分体元と前記第 2 の選択回路により選択された部分体元との積を演算する部分体乗算回路と、

前記第 1 の元および前記第 2 の元の積に対応する前記部分体の 2 つの元のうちの一方となる前記部分体の元を記憶する第 1 の記憶回路と、

前記第 1 の元および前記第 2 の元の積に対応する前記部分体の 2 つの元のうちの他方となる前記部分体の元を記憶する第 2 の記憶回路と、

前記第 1 の記憶回路に記憶された前記部分体の元と前記部分体乗算回路による積との和を演算する第 3 の部分体加算回路と、

前記第 2 の記憶回路に記憶された前記部分体の元と前記部分体乗算回路による積との和を演算する第 4 の部分体加算回路と、

所定のタイミングにおいて前記第 3 の部分体加算回路による和で、前記第 1 の記憶回路に記憶された前記部分体の元を更新する第 1 の更新回路と、

所定のタイミングにおいて前記第 4 の部分体加算回路による和で、前記第 2 の記憶回路に記憶された前記部分体の元を更新する第 2 の更新回路とを備えることを特徴とするガロア体乗算回路。

【請求項 2】 第 1 の記憶回路および第 2 の記憶回路は初期値として 0 を記憶し、

第 1 の選択回路は、第 1 のタイミングで第 1 の部分体元を選択し、第 2 のタイミングで第 2 の部分体元を選択し、第 3 のタイミングで第 3 の部分体元を選択し、

第 2 の選択回路は、前記第 1 のタイミングで第 4 の部分体元を選択し、前記第 2 のタイミングで第 5 の部分体元を選択し、前記第 3 のタイミングで第 6 の部分体元を選択し、

第 1 の更新回路は、前記第 1 のタイミングおよび前記第

2

2 のタイミングで更新し、

第 2 の更新回路は、前記第 1 のタイミングおよび前記第 3 のタイミングで更新することを特徴とする請求項 1 記載のガロア体乗算回路。

【請求項 3】 n を自然数とし、

第 1 の選択回路は、第 1 の部分体元、第 2 の部分体元、第 3 の部分体元、およびガロア体 $GF(2^{2n})$ から部分体 $GF(2^n)$ へのノルムである第 7 の部分体元のうちのいずれかを選択し、

第 2 の選択回路は、第 4 の部分体元、第 5 の部分体元、第 6 の部分体元、および部分体乗算回路による積のうちのいずれかを選択することを特徴とする請求項 1 記載のガロア体乗算回路。

【請求項 4】 第 1 の記憶回路および第 2 の記憶回路は初期値として 0 を記憶し、

第 1 の選択回路は、第 4 のタイミングで第 1 の部分体元を選択し、第 5 のタイミングで第 2 の部分体元を選択した後に第 6 のタイミングで第 7 の部分体元を選択し、第 7 のタイミングで第 3 の部分体元を選択し、

第 2 の選択回路は、前記第 4 のタイミングで第 4 の部分体元を選択し、前記第 5 のタイミングで第 5 の部分体元を選択した後に前記第 6 のタイミングで、前記第 5 のタイミングにおける部分体乗算回路による積を選択し、前記第 7 のタイミングで第 6 の部分体元を選択し、

第 1 の更新回路は、前記第 4 のタイミングおよび前記第 6 のタイミングで更新し、

第 2 の更新回路は、前記第 4 のタイミングおよび前記第 7 のタイミングで更新することを特徴とする請求項 3 記載のガロア体乗算回路。

【請求項 5】 ガロア体の元の逆元を演算するガロア体逆元演算回路において、

n を奇数とするガロア体 $GF(2^{2n})$ の部分体 $GF(2^n)$ の元であって前記ガロア体 $GF(2^{2n})$ の元に対応する第 1 の部分体元および第 2 の部分体元の和を第 8 の部分体元として演算する第 5 の部分体加算回路と、

前記第 2 の部分体元および前記第 8 の部分体元のうちのいずれかを選択する第 3 の選択回路と、

前記部分体 $GF(2^n)$ の元の逆元を演算する部分体逆元回路と、

前記第 1 の部分体元、前記第 2 の部分体元、および前記部分体逆元回路による逆元のうちのいずれかを選択する第 4 の選択回路と、

前記第 3 の選択回路により選択された部分体元と前記第 4 の選択回路により選択された部分体元との積を演算する部分体乗算回路と、

所定のタイミングでの前記部分体乗算回路による積を記憶または累積し、前記部分体逆元回路に供給する記憶累積回路と、

前記部分体 $GF(2^n)$ の元であって前記ガロア体 $GF(2^{2n})$ の元の逆元に対応する第 9 の部分体元および第

50

3

10の部分体元のうちの前記第9の部分体元として、所定のタイミングにおいて前記部分体乗算回路による積を出力する第1の出力回路と、

前記第10の部分体元として、所定のタイミングにおいて前記部分体乗算回路による積を出力する第2の出力回路とを備えることを特徴とするガロア体逆元演算回路。

【請求項6】 第3の選択回路は、第8のタイミングで第2の部分体元を選択し、第9のタイミングで第8の部分体元を選択し、第10のタイミングで第8の部分体元を選択し、第11のタイミングで第2の部分体元を選択し、

第4の選択回路は、前記第8のタイミングで前記第2の部分体元を選択し、前記第9のタイミングで第1の部分体元を選択し、前記第10のタイミングおよび第11のタイミングで部分体逆元回路による逆元を選択し、

記憶累積回路は、前記第8のタイミングで前記部分体乗算回路による積を記憶し、前記第9のタイミングでその記憶した値を前記部分体逆元回路に供給した後に前記部分体乗算回路による積を累積記憶し、前記第10のタイミングおよび第11のタイミングでその累積記憶した値を前記部分体逆元回路に供給し、

第1の出力回路は、前記第10のタイミングで出力し、第2の出力回路は、前記第11のタイミングで出力することを特徴とする請求項5記載のガロア体逆元演算回路。

【請求項7】 n を自然数とし、

第3の選択回路は、第2の部分体元、第8の部分体元、およびガロア体 $GF(2^{2n})$ から部分体 $GF(2^n)$ へのノルムである第11の部分体元のうちのいずれかを選択し、

第4の選択回路は、第1の部分体元、第2の部分体元、部分体逆元回路による逆元、および記憶累積回路に記憶または累積された値のうちのいずれかを選択することを特徴とする請求項5記載のガロア体逆元演算回路。

【請求項8】 第3の選択回路は、第12のタイミングで第2の部分体元を選択し、第13のタイミングで第11の部分体元を選択し、第14のタイミングおよび第15のタイミングで第8の部分体元を選択し、第16のタイミングで前記第2の部分体元を選択し、

第4の選択回路は、前記第12のタイミングで前記第2の部分体元を選択し、前記第13のタイミングで記憶累積回路の記憶値を選択し、前記第14のタイミングで第1の部分体元を選択し、前記第15のタイミングおよび前記第16のタイミングで部分体逆元回路による逆元を選択し、

記憶累積回路は、前記第12のタイミングで前記部分体乗算回路による積を記憶し、前記第13のタイミングでその記憶した値を前記第4の選択回路に供給した後に前記部分体乗算回路による積を記憶し、前記第14のタイミングで前記部分体乗算回路による積を累積記憶し、前

4

記第15のタイミングおよび前記第16のタイミングでその累積記憶した値を前記部分体逆元回路に供給し、第1の出力回路は、前記第15のタイミングで出力し、第2の出力回路は、前記第16のタイミングで出力することを特徴とする請求項7記載のガロア体逆元演算回路。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、例えば符号化器や復号化器において、ガロア体の乗算や逆元演算などのガロア体演算を実行するガロア体乗算回路およびガロア体逆元演算回路に関するものである。

【0002】

【従来の技術】ガロア体の演算は誤り訂正符号の符号化や復号化において必要とされることが多く、様々な演算方法や演算回路が提案されている。特に基礎体 GF

(2) 上の偶数次ガロア拡大体 $GF(2^{2n})$ での演算

を、その部分体 $GF(2^n)$ での演算により実現する方法が、例えば特開平1-181232号公報、「有限体 $GF(2^{2n})$ 演算回路に関する一検討」(松井ら著、電子情報通信学会信学技報IT88-14)(以下、文献1という)、「 $GF(2^n)$ における逆元の高速算法について」(森井、笠原著、電子情報通信学会信学技報IT87-24)および「 $GF(2^n)$ における逆元の高速算法について [II]」(森井、笠原著、電子情報通信学会信学技報IT87-54)に提案されている。

【0003】このうちの例えば文献1を参照して、ガロア体 $GF(2^{2n})$ での演算とその部分体 $GF(2^n)$ の演算との関係について説明する。

【0004】 n を自然数とするガロア体 $GF(2^{2n})$

(以下、 K という) は部分体 $GF(2^n)$ (以下、 L という) を包含し、このガロア体 K は部分体 L の2次拡大体になる。ここで部分体 L に属さないガロア体 K の元 a を選ぶと、集合 $\{1, a\}$ は部分体 L 上のガロア体 K の基底となる。ガロア体 K の元 x は、この基底および部分体 L の2つの元 x_0, x_1 に基づいて $x = x_0 + x_1 \times a$ と一意的に表される。また、元 a は $a^2 + T(a) \times a + N(a) = 0$ なる関係式を満たし、さらに a として $T(a) = 1$ を満たすものを選ぶ。ただし、次のように $T(a)$ は元 a のガロア体 K から部分体 L へのトレースを表し、 $N(a)$ はガロア体 K の元 a のガロア体 K から部分体 L へのノルムを表す。

$$T(a) = a + a^{2^n}, \quad N(a) = a^{2^{n+1}}$$

【0005】そしてガロア体 K の演算は上述の基底上では部分体 L の演算に分解することができる。

【0006】まず、ガロア体 K の元 x と元 y との加算について説明する。上述のように、ガロア体 K の元 x, y を部分体 L の元 x_0, x_1, y_0, y_1 で表すと次に示すようになる。

5

$$x = x_0 + x_1 \times a$$

$$y = y_0 + y_1 \times a$$

【0007】したがってガロア体Kの元xと元yとの加算は、次に示すように、部分体Lの加算に分解される。

$$x + y = x_0 + y_0 + (x_1 + y_1) \times a$$

【0008】次にガロア体Kの元xと元yとの乗算について説明する。ガロア体Kの元x, yを同様に部分体Lの元 x_0, x_1, y_0, y_1 で表すと、ガロア体Kの元xと元yとの乗算は、部分体Lでの加算、乗算およびノルム倍乗算に分解される。なお、部分体Lの元に対する「-1」の乗算は「+1」の乗算と等価であるため、ガロア体Kの元xと元yとの乗算は次に示すようになる。

$$x \times y = x_0 \times y_0 + N(a) \times x_1 \times y_1 + \{ (x_0 + x_1) \times (y_0 + y_1) + x_0 \times y_0 \} \times a$$

【0009】同様に、ガロア体Kの元xの逆元 x^{-1} は、次に示すように、部分体Lでの加算、2乗演算、乗算、逆元演算およびノルム倍乗算により計算される。

$$x^{-1} = \{ x_0 \times (x_0 + x_1) + N(a) \times x_1^2 \}^{-1} \times (x_0 + x_1) + \{ x_0 \times (x_0 + x_1) + N(a) \times x_1^2 \}^{-1} \times x_1 \times a$$

【0010】このように、ガロア体Kでの加算、乗算および逆元演算は、その部分体Lでの演算に置き換えることができる。

【0011】図5は、例えば文献1に記載の従来のガロア体乗算回路を示すブロック図である。図において、151A~151Dはガロア体Kの部分体Lの2つの元の和をそれぞれ計算する部分体加算回路であり、152A~152Cはガロア体Kの部分体Lの2つの元の積をそれぞれ計算する部分体乗算回路であり、153は所定の基底{1, a}に基づいて、部分体Lの元に、ガロア体Kの元aについてのノルム $N(a)$ を乗算するノルム乗算回路である。

【0012】次に動作について説明する。まず、ガロア体Kの元xに対応する部分体Lの2つの元 x_0, x_1 が部分体加算回路151Aに供給され、ガロア体Kの元yに対応する部分体Lの2つの元 y_0, y_1 が部分体加算回路151Bに供給される。また、部分体元 x_1, y_1 が部分体乗算回路152Aに供給され、部分体元 x_0, y_0 が部分体乗算回路152Bに供給される。

【0013】そして部分体加算回路151Aは、供給された2つの部分体元 x_0, x_1 の和 $(x_0 + x_1)$ を計算して部分体乗算回路152Cに供給し、部分体加算回路151Bは、供給された2つの部分体元 y_0, y_1 の和 $(y_0 + y_1)$ を計算して部分体乗算回路152Cに供給する。部分体乗算回路152Cは、供給された部分体元 $(x_0 + x_1), (y_0 + y_1)$ の積 $(x_0 + x_1) \times (y_0 + y_1)$ を計算して部分体加算回路151Dに供給する。

【0014】一方、部分体乗算回路152Aは、供給された2つの部分体元 x_1, y_1 の積 $(x_1 \times y_1)$ を計

6

算してノルム乗算回路153に供給する。ノルム乗算回路153は、供給された部分体元 $(x_1 \times y_1)$ にノルム $N(a)$ を乗算し、その演算結果 $(x_1 \times y_1 \times N(a))$ を部分体加算回路151Cに供給する。また部分体乗算回路152Bは、供給された2つの部分体元 x_0, y_0 の積 $(x_0 \times y_0)$ を計算して部分体加算回路151C, 151Dに供給する。

【0015】そして、部分体加算回路151Cは、供給された2つの部分体 $(x_1 \times y_1 \times N(a))$, $(x_0 \times y_0)$ の和を計算し、ガロア体Kの元x, yの積zを基底{1, a}で分解した際 $(z = z_0 + z_1 \times a)$ の部分体Lの元 $z_0 (= x_0 \times y_0 + x_1 \times y_1 \times N(a))$ として出力する。また、部分体加算回路151Dは、供給された2つの部分体 $(x_0 + x_1) \times (y_0 + y_1)$, $(x_0 \times y_0)$ の和を計算し、ガロア体Kの元x, yの積zを基底{1, a}で分解した際 $(z = z_0 + z_1 \times a)$ の部分体Lの元 $z_1 (= x_0 \times y_0 + (x_0 + x_1) \times (y_0 + y_1))$ として出力する。

【0016】このようにしてガロア体Kの元x, yの積zが演算される。

【0017】また、図6は、例えば文献1に記載の従来のガロア体逆元演算回路を示すブロック図である。図において、161Aおよび161Bはガロア体Kの部分体Lの2つの元の和をそれぞれ計算する部分体加算回路であり、162A~162Cはガロア体Kの部分体Lの2つの元の積をそれぞれ計算する部分体乗算回路であり、163は部分体Lの元の2乗を演算する部分体2乗回路であり、164は所定の基底{1, a}に基づいて、部分体Lの元に、ガロア体Kの元aについてのノルム $N(a)$ を乗算するノルム乗算回路であり、165は部分体Lの元の逆元を演算する逆元回路である。

【0018】次に動作について説明する。まず、ガロア体Kの元xに対応する部分体Lの2つの元 x_0, x_1 が部分体加算回路161Aに供給され、さらに、部分体元 x_0 が部分体乗算回路162Aに供給され、部分体元 x_1 が部分体乗算回路162Cおよび部分体2乗回路163に供給される。

【0019】そして部分体加算回路161Aは、供給された2つの部分体元 x_0, x_1 の和 $(x_0 + x_1)$ を計算して部分体乗算回路162A, 162Bに供給し、部分体乗算回路162Aは、供給された部分体元 x_0 と部分体元 $(x_0 + x_1)$ との積 $(x_0 \times (x_0 + x_1))$ を計算して部分体加算回路161Bに供給する。

【0020】一方、部分体2乗回路163は、供給された部分体元 x_1 の2乗を計算してノルム乗算回路164に供給する。ノルム乗算回路164は、供給された部分体元 (x_1^2) にノルム $N(a)$ を乗算し、その演算結果 $(x_1^2 \times N(a))$ を部分体加算回路161Bに供給する。

【0021】そして、部分体加算回路161Bは、供給

7

された2つの部分体 $(x_1^2 \times N(a))$, $(x_0 \times (x_0 + x_1))$ の和 $(x_0 \times (x_0 + x_1) + x_1^2 \times N(a))$ を計算し、逆元回路165に供給する。逆元回路165は供給された部分体元 $(x_0 \times (x_0 + x_1) + x_1^2 \times N(a))$ の逆元を演算し、部分体乗算回路162B, 162Cに供給する。

【0022】部分体乗算回路162Bは、部分体加算回路161Aからの部分体元 $(x_0 + x_1)$ と逆元回路165からの部分体元 $(\{x_0 \times (x_0 + x_1) + x_1^2 \times N(a)\}^{-1})$ との積を計算し、ガロア体Kの元xの逆元zを基底 $\{1, a\}$ で分解した際 $(z = z_0 + z_1 \times a)$ の部分体Lの元 $z_0 (= (x_0 + x_1) \times \{x_0 \times (x_0 + x_1) + x_1^2 \times N(a)\}^{-1})$ として出力する。

【0023】同様に、部分体乗算回路162Cは、供給された部分体元 x_1 と逆元回路165からの部分体元 $(\{x_0 \times (x_0 + x_1) + x_1^2 \times N(a)\}^{-1})$ との積を計算し、ガロア体Kの元xの逆元zを基底 $\{1, a\}$ で分解した際 $(z = z_0 + z_1 \times a)$ の部分体Lの元 $z_1 (= x_1 \times \{x_0 \times (x_0 + x_1) + x_1^2 \times N(a)\}^{-1})$ として出力する。

【0024】このようにしてガロア体Kの元xの逆元zが演算される。

【0025】なお、その他の従来の技術としては、例えば特開平2-217022号公報、特開平6-314979号公報、特開平9-305572号公報に記載のガロア体演算回路がある。

【0026】

【発明が解決しようとする課題】従来のガロア体乗算回路およびガロア体逆元演算回路は以上のように構成されているので、部分体元のための演算回路が多く必要になり、全体の回路規模を低減することが困難であるなどの課題があった。

【0027】例えば上述の従来のガロア体乗算回路では、3個の部分体乗算回路、4個の部分体加算回路および1個のノルム乗算回路で構成されており、特に他の部分体演算回路に比較して回路量が多い部分体乗算回路が多く使用されるため、全体での回路規模が大きくなってしまふ。また上述の従来のガロア体逆元演算回路では、3個の部分体乗算回路、2個の部分体加算回路、1個の部分体2乗回路、1個のノルム乗算回路および1個の逆元回路で構成されており、部分体乗算回路が多く使用されるため、全体での回路規模が大きくなってしまふ。

【0028】また、部分体演算回路はいずれもAND回路とEXOR回路で構成される組合せ回路であるため、部分体演算回路を直列／並列に多数接続して構成され、入力から出力までの遅延が大きくなり演算速度を高くすることが困難であるという課題があった。

【0029】この発明は上記のような課題を解決するためになされたもので、主に部分体乗算回路の数を少なく

8

するようにして、全体での回路規模を低減するとともに、演算速度を高くすることができるガロア体乗算回路およびガロア体逆元演算回路を得ることを目的とする。

【0030】

【課題を解決するための手段】この発明に係るガロア体乗算回路は、ガロア体 $GF(2^{2n})$ (n は奇数) の部分体 $GF(2^n)$ の元であってガロア体 $GF(2^{2n})$ の第1の元に対応する第1の部分体元および第2の部分体元の和を第3の部分体元として演算する第1の部分体加算回路と、部分体の元であってガロア体 $GF(2^{2n})$ の第2の元に対応する第4の部分体元と第5の部分体元との和を第6の部分体元として演算する第2の部分体加算回路と、第1の部分体元、第2の部分体元および第3の部分体元のうちのいずれかを選択する第1の選択回路と、第4の部分体元、第5の部分体元および第6の部分体元のうちのいずれかを選択する第2の選択回路と、第1の選択回路により選択された部分体元と第2の選択回路により選択された部分体元との積を演算する部分体乗算回路と、第1の元および第2の元の積に対応する部分体の2つの元のうち的一方となる部分体の元を記憶する第1の記憶回路と、第1の元および第2の元の積に対応する部分体の2つの元のうち他方となる部分体の元を記憶する第2の記憶回路と、第1の記憶回路に記憶された部分体の元と部分体乗算回路による積との和を演算する第3の部分体加算回路と、第2の記憶回路に記憶された部分体の元と部分体乗算回路による積との和を演算する第4の部分体加算回路と、所定のタイミングにおいて第3の部分体加算回路による和で、第1の記憶回路に記憶された部分体の元を更新する第1の更新回路と、所定のタイミングにおいて第4の部分体加算回路による和で、第2の記憶回路に記憶された部分体の元を更新する第2の更新回路とを備えるものである。

【0031】この発明に係るガロア体乗算回路は、第1の記憶回路および第2の記憶回路に初期値として0を記憶し、第1のタイミングで、第1の選択回路が第1の部分体元を選択するとともに第2の選択回路が第4の部分体元を選択し、第1および第2の更新回路が更新をし、第2のタイミングで、第1の選択回路が第2の部分体元を選択するとともに第2の選択回路が第5の部分体元を選択し、第1の更新回路が更新をし、第3のタイミングで、第1の選択回路が第3の部分体元を選択するとともに第2の選択回路が第6の部分体元を選択し、第2の更新回路が更新するようにしたものである。

【0032】この発明に係るガロア体乗算回路は、 n を自然数とし、第1の選択回路が第1の部分体元、第2の部分体元、第3の部分体元、およびガロア体 $GF(2^{2n})$ から部分体 $GF(2^n)$ へのノルムである第7の部分体元の中のいずれかを選択し、第2の選択回路が第4の部分体元、第5の部分体元、第6の部分体元、および部分体乗算回路による積の中のいずれかを選択

9

するようにしたものである。

【0033】この発明に係るガロア体乗算回路は、第1の記憶回路および第2の記憶回路に初期値として0を記憶し、第4のタイミングで、第1の選択回路が第1の部分体元を選択するとともに第2の選択回路が第4の部分体元を選択し、第1の更新および第2の更新回路が更新をし、第5のタイミングで、第1の選択回路が第2の部分体元を選択し、第2の選択回路が第5の部分体元を選択した後に第6のタイミングで、第1の選択回路が第7の部分体元を選択するとともに第2の選択回路が第5の10のタイミングにおける部分体乗算回路による積を選択し、第1の更新回路が更新をし、第7のタイミングで、第1の選択回路が第3の部分体元を選択するとともに第2の選択回路が第6の部分体元を選択し、第2の更新回路が更新をするようにしたものである。

【0034】この発明に係るガロア体逆元演算回路は、ガロア体 $GF(2^n)$ (n は奇数) の部分体 GF

(2^n) の元であってガロア体 $GF(2^n)$ の元に対応する第1の部分体元および第2の部分体元の和を第8の部分体元として演算する第5の部分体加算回路と、第2の部分体元および第8の部分体元のうちのいずれかを選択する第3の選択回路と、部分体 $GF(2^n)$ の元の逆元を演算する部分体逆元回路と、第1の部分体元、第2の部分体元、および部分体逆元回路による逆元のうちの11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000

【0035】この発明に係るガロア体逆元演算回路は、第8のタイミングで、第3の選択回路が第2の部分体元を選択するとともに第4の選択回路が第2の部分体元を選択し、記憶累積回路が部分体乗算回路による積を記憶し、第9のタイミングで、第3の選択回路が第8の部分体元を選択するとともに第4の選択回路が第1の部分体元を選択し、記憶累積回路が記憶している値を部分体逆元回路に供給した後に部分体乗算回路による積を累積記憶し、第10のタイミングで、第3の選択回路が第8の部分体元を選択するとともに第4の選択回路が部分体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第1の出力回路が出力をし、第11のタイミングで、第3の選択回路が第2の部分体元を選択するとともに第4の選択回路が部分

10

体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第2の出力回路が出力をするようにしたものである。

【0036】この発明に係るガロア体逆元演算回路は、 n を自然数とし、第3の選択回路が第2の部分体元、第8の部分体元、およびガロア体 $GF(2^n)$ から部分体 $GF(2^n)$ へのノルムである第11の部分体元のうちのいずれかを選択し、第4の選択回路が第1の部分体元、第2の部分体元、部分体逆元回路による逆元、および記憶累積回路に記憶または累積された値のうちのいずれかを選択するようにしたものである。

【0037】この発明に係るガロア体逆元演算回路は、第12のタイミングで、第3の選択回路が第2の部分体元を選択するとともに第4の選択回路が第2の部分体元を選択し、記憶累積回路が部分体乗算回路による積を記憶し、第13のタイミングで、第3の選択回路が第11の部分体元を選択するとともに第4の選択回路が記憶累積回路の記憶値を選択し、記憶累積回路が記憶している値を第4の選択回路に供給した後に部分体乗算回路による積を記憶し、第14のタイミングで、第3の選択回路が第8の部分体元を選択するとともに第4の選択回路が第1の部分体元を選択し、記憶累積回路が部分体乗算回路による積を累積記憶し、第15のタイミングで、第3の選択回路が第8の部分体元を選択するとともに第4の選択回路が部分体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第1の出力回路が出力をし、第16のタイミングで、第3の選択回路が第2の部分体元を選択するとともに第4の選択回路が部分体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第2の出力回路が出力をするようにしたものである。

【0038】

【発明の実施の形態】以下、この発明の実施の一形態を説明する。

実施の形態1. この発明の実施の形態1によるガロア体乗算回路は、 n を奇数とするガロア体 $GF(2^n)$ の2つの元 x 、 y の積 z を演算するものである。図1は、この発明の実施の形態1によるガロア体乗算回路の構成を示すブロック図である。

【0039】図において、1Aおよび1Bは、 n を奇数とするガロア体 $GF(2^n)$ の部分体 $GF(2^n)$ の元であってガロア体 $GF(2^n)$ の元 x (第1の元) ($=x_0 + x_1 \times \beta$ 、 β は部分体 $GF(2^n)$ に属さないガロア体 $GF(2^n)$ の元) に対応する部分体元 x_0 (第1の部分体元) および部分体元 x_1 (第2の部分体元) をそれぞれ供給され記憶する記憶回路であり、2は記憶回路1Aに記憶された部分体元 x_0 および記憶回路1Bに記憶された部分体元 x_1 の和を演算する第1の部分体加算回路であり、3は記憶回路1Aに記憶された部分体

11

元 x_0 、記憶回路1Bに記憶された部分体元 x_1 および第1の部分体加算回路2の演算結果である部分体元 $(x_0 + x_1)$ (第3の部分体元)のうちのいずれかを選択する第1の選択回路である。

【0040】4Aおよび4Bは、 n を奇数とするガロア体 $GF(2^{2n})$ の部分体 $GF(2^n)$ の元であってガロア体 $GF(2^{2n})$ の元 y (第2の元) $(=y_0 + y_1 \times \beta)$ に対応する部分体元 y_0 (第3の部分体元)および部分体元 y_1 (第4の部分体元)をそれぞれ供給され記憶する記憶回路であり、5は記憶回路4Aに記憶された部分体元 y_0 および記憶回路4Bに記憶された部分体元 y_1 の和を演算する第2の部分体加算回路であり、6は記憶回路4Aに記憶された部分体元 y_0 、記憶回路4Bに記憶された部分体元 y_1 および第2の部分体加算回路5の演算結果である部分体元 $(y_0 + y_1)$ (第6の部分体元)のうちのいずれかを選択する第2の選択回路である。

【0041】7は第1の選択回路3により選択された部分体元と第2の選択回路6により選択された部分体元との積を演算する部分体乗算回路である。8Aは記憶回路10Aに記憶された部分体元と部分体乗算回路7による積との和を演算する第3の部分体加算回路であり、8Bは記憶回路10Bに記憶された部分体元と部分体乗算回路7による積との和を演算する第4の部分体加算回路である。9Aは所定のタイミングにおいてオン状態になり、第3の部分体加算回路8Aによる和で、記憶回路10Aに記憶された部分体元を更新するスイッチ回路 (第1の更新回路)であり、9Bは所定のタイミングにおいてオン状態になり、第4の部分体加算回路8Bによる和で、記憶回路10Bに記憶された部分体元を更新するス

イッチ回路 (第2の更新回路)である。

【0042】10Aは元 x および元 y の積 $z (=z_0 + z_1 \times \beta)$ に対応する部分体 $GF(2^n)$ の2つの元 z_0 、 z_1 のうちの一方 (z_0)に最終的になる部分体元を記憶する記憶回路 (第1の記憶回路)であり、10Bは元 x および元 y の積 $z (=z_0 + z_1 \times \beta)$ に対応する部分体 $GF(2^n)$ の2つの元 z_0 、 z_1 のうちの他方 (z_1)に最終的になる部分体元を記憶する記憶回路 (第2の記憶回路)である。

【0043】なお、 n が奇数である場合、ガロア体 $GF(2^{2n})$ の上述の元 β のノルム $N(\beta)$ は1とすることができ、元 x 、 y の積の演算のためにノルム $N(\beta)$ 倍乗算は必要ない。ここで、一例として n が7である場合について説明する。ガロア体 $GF(2^{14})$ の原始多項式を $x^{14} + x^{10} + x^6 + x + 1$ とし、その根 (ガロア体 $GF(2^{14})$ の原始元)を α とする。 $\gamma = \alpha^{129}$ とおくと γ は原始多項式 $x^7 + x + 1$ の根であり、 γ より生成される部分体はガロア体 $GF(2^7)$ になる。また、 $\beta = \alpha^{5461}$ とすると、 β は部分体 $GF(2^7)$ に属さないためガロア体 $GF(2^{14})$ は β および γ により生

12

成され、集合 $\{\beta\gamma^6, \beta\gamma^5, \beta\gamma^4, \beta\gamma^3, \beta\gamma^2, \beta\gamma, \beta, \gamma^6, \gamma^5, \gamma^4, \gamma^3, \gamma^2, \gamma, 1\}$ はガロア体 $GF(2^{14})$ の基礎体上の基底となる。このとき、 $\beta^3 = 1$ なる関係を満たすので β についてのトレース $T(\beta)$ とノルム $N(\beta)$ は1となる。

【0044】次に動作について説明する。この実施の形態1によるガロア体乗算回路は、 n を奇数とするガロア体 $GF(2^{2n})$ の2つの元 $x (=x_0 + x_1 \times \beta)$ 、 $y (=y_0 + y_1 \times \beta)$ の積 $z (=z_0 + z_1 \times \beta)$ を3ステップで計算する。

【0045】まず、記憶回路1A、1Bに部分体元 x_0 、 x_1 がそれぞれ供給、記憶され、記憶回路4A、4Bに部分体元 y_0 、 y_1 がそれぞれ供給、記憶され、記憶回路10A、10Bに初期値0が記憶される。

【0046】第1のステップ (第1のタイミング)では、スイッチ回路9A、9Bがオン状態に制御され、第1の選択回路3が部分体元 x_0 を選択するとともに第2の選択回路6が部分体元 y_0 を選択する。したがって部分体乗算回路7に部分体元 x_0 と部分体元 y_0 とが供給され、それらの積 $(x_0 \times y_0)$ が部分体乗算回路7により計算され、部分体加算回路8A、8Bに供給される。

【0047】そして、部分体加算回路8A、8Bは、記憶回路10A、10Bに記憶された値 (今の場合、初期値0)と部分体乗算回路7による積 $(x_0 \times y_0)$ との和をそれぞれ計算し、スイッチ回路9A、9Bを介して記憶回路10A、10Bにそれぞれ記憶させる。

【0048】次に第2のステップ (第2のタイミング)では、スイッチ回路9Aがオン状態に制御されるとともにスイッチ回路9Bがオフ状態に制御され、第1の選択回路3が部分体元 x_1 を選択するとともに第2の選択回路6が部分体元 y_1 を選択する。したがって部分体乗算回路7に部分体元 x_1 と部分体元 y_1 とが供給され、それらの積 $(x_1 \times y_1)$ が部分体乗算回路7により計算され、部分体加算回路8A、8Bに供給される。

【0049】そして、部分体加算回路8A、8Bは、記憶回路10A、10Bに記憶された値 (今の場合、 $x_0 \times y_0$)と部分体乗算回路7による積 $(x_1 \times y_1)$ との和をそれぞれ計算する。今、スイッチ回路9Aだけがオン状態であるので、部分体加算回路8Aによる和 $(x_0 \times y_0 + x_1 \times y_1)$ がスイッチ回路9Aを介して記憶回路10Aに記憶される。なお、記憶回路10Bには、そのまま、部分体元 $(x_0 \times y_0)$ が保持される。

【0050】最後に第3のステップ (第3のタイミング)では、スイッチ回路9Aがオフ状態に制御されるとともにスイッチ回路9Bがオン状態に制御され、第1の選択回路3が部分体元 $(x_0 + x_1)$ を選択するとともに第2の選択回路6が部分体元 $(y_0 + y_1)$ を選択する。したがって部分体乗算回路7に部分体元 $(x_0 + x_1)$ と部分体元 $(y_0 + y_1)$ とが供給され、それらの

13

積 $((x_0 + x_1) \times (y_0 + y_1))$ が部分体乗算回路7により計算され、部分体加算回路8A、8Bに供給される。

【0051】そして、部分体加算回路8Aは、記憶回路10Aに記憶された値（今の場合、 $(x_0 \times y_0 + x_1 \times y_1)$ ）と部分体乗算回路7による積 $((x_0 + x_1) \times (y_0 + y_1))$ との和を計算し、部分体加算回路8Bは、記憶回路10Bに記憶された値（今の場合、 $x_0 \times y_0$ ）と部分体乗算回路7による積 $((x_0 + x_1) \times (y_0 + y_1))$ との和を計算する。今、スイッチ回路9Bだけがオン状態であるので、部分体加算回路8Bによる和 $(x_0 \times y_0 + (x_0 + x_1) \times (y_0 + y_1))$ がスイッチ回路9Bを介して記憶回路10Bに記憶される。なお、記憶回路10Aには、そのまま、部分体元 $(x_0 \times y_0 + x_1 \times y_1)$ が保持される。

【0052】このようにして第1～第3のステップの処理により、元xおよび元yの積 $z (= z_0 + z_1 \times \beta)$ に対応する部分体GF (2^n) の元 $z_0 (= x_0 \times y_0 + x_1 \times y_1)$ が記憶回路10Aに記憶され、また出力され、部分体GF (2^n) の元 $z_1 (= x_0 \times y_0 + (x_0 + x_1) \times (y_0 + y_1))$ が記憶回路10Bに記憶され、出力される。なお、スイッチ回路9A、9Bおよび第1および第2の選択回路3、6の制御は、最終的に記憶回路10A、10Bに記憶される値が上述のようになれば他の方式でもよい。

【0053】以上のように、この実施の形態1によれば、nが奇数であるガロア体GF (2^{2n}) についてのガロア体乗算回路における部分体演算回路を1個の部分体乗算回路および4個の部分体加算回路としたので、その他に選択回路、スイッチ回路などが必要になるものの、全体の回路規模を低減することができるという効果が得られる。

【0054】また、演算を3つのステップに分割し、部分体演算のうち出力遅延の大きい部分体乗算を各ステップにおいて1回だけ実行するようにしたので、乗算全体での出力遅延が低減され、演算を高速に実行することができるという効果が得られる。

【0055】実施の形態2。この発明の実施の形態2によるガロア体乗算回路は、nを自然数とするガロア体GF (2^{2n}) の2つの元x、yの積zを演算するものである。図2は、この発明の実施の形態2によるガロア体乗算回路の構成を示すブロック図である。

【0056】図において、3Aは記憶回路1Aに記憶された部分体元 x_0 、記憶回路1Bに記憶された部分体元 x_1 、第1の部分体加算回路2の演算結果である部分体元 $(x_0 + x_1)$ および記憶回路21に記憶されたノルムN (β) (第7の部分体元) のうちのいずれかを選択する第1の選択回路である。

【0057】6Aは記憶回路4Aに記憶された部分体元

14

y_0 、記憶回路4Bに記憶された部分体元 y_1 、第2の部分体加算回路5の演算結果である部分体元 $(= y_0 + y_1)$ および記憶回路23に記憶された部分体元のうちのいずれかを選択する第2の選択回路である。

【0058】21は元x、yと部分体元 x_0 、 x_1 、 y_0 、 y_1 との対応関係 $(x = x_0 + x_1 \times \beta, y = y_0 + y_1 \times \beta)$ を示す部分体GF (2^n) に属さないガロア体GF (2^{2n}) の元 β についてのガロア体GF

(2^{2n}) から部分体GF (2^n) へのノルムN (β) を供給され記憶する記憶回路であり、22は部分体乗算回路7による積の供給先を所定のタイミングで切り換えるスイッチ回路であり、23はスイッチ回路22を介して供給された部分体乗算回路7による積を記憶する記憶回路である。

【0059】なお、図2におけるその他の構成要素については実施の形態1によるもの（図1）と同様であるのでその説明を省略する。また、ノルムN (β) は図示せぬ所定の演算回路により演算され供給される。

【0060】なお、nが自然数である場合、ガロア体GF (2^{2n}) の上述の元 β のノルムN (β) が1とは限らない。ここでnが4である場合について説明する。ガロア体GF (2^8) の原始多項式を $x^8 + x^6 + x^5 + x^3 + 1$ とし、その根（ガロア体GF (2^8) の原始元）を β とする。 $\gamma = \beta^{238}$ とすると γ は原始多項式 $x^4 + x + 1$ の根であり、 γ より生成される部分体はガロア体GF (2^4) になる。ガロア体GF (2^8) は β および γ より生成され、集合 $\{\beta \gamma^3, \beta \gamma^2, \beta \gamma, \beta, \gamma^3, \gamma^2, \gamma, 1\}$ はガロア体GF (2^8) の基礎体上の基底となる。この場合のノルムN (β) は $\beta^{17} (= \gamma^{14})$ である。

【0061】次に動作について説明する。この実施の形態2によるガロア体乗算回路は、nを自然数とするガロア体GF (2^{2n}) の2つの元x $(= x_0 + x_1 \times \beta)$ 、y $(= y_0 + y_1 \times \beta)$ の積z $(= z_0 + z_1 \times \beta)$ を4ステップで計算する。

【0062】まず、記憶回路1A、1Bに部分体元 x_0 、 x_1 がそれぞれ供給、記憶され、記憶回路4A、4Bに部分体元 y_0 、 y_1 がそれぞれ供給、記憶され、記憶回路21にノルムN (β) が供給、記憶され、記憶回路10A、10Bに初期値0が記憶される。

【0063】第1のステップ（第4のタイミング）では、スイッチ回路9A、9Bがオン状態に制御されるとともにスイッチ回路22が部分体乗算回路7と部分体加算回路8A、8Bとを電氣的に接続し、第1の選択回路3Aが部分体元 x_0 を選択するとともに第2の選択回路6Aが部分体元 y_0 を選択する。したがって部分体乗算回路7に部分体元 x_0 と部分体元 y_0 とが供給され、それらの積 $(x_0 \times y_0)$ が部分体乗算回路7により計算され、スイッチ回路22を介して部分体加算回路8A、8Bに供給される。

15

【0064】そして、部分体加算回路8A、8Bは、記憶回路10A、10Bに記憶された値（今の場合、初期値0）と部分体乗算回路7による積（ $x_0 \times y_0$ ）との和をそれぞれ計算し、記憶回路10A、10Bに記憶させる。

【0065】次に第2のステップ（第5のタイミング）では、スイッチ回路22が部分体乗算回路7と記憶回路23とを電氣的に接続し、第1の選択回路3Aが部分体元 x_1 を選択するとともに第2の選択回路6Aが部分体元 y_1 を選択する。したがって部分体乗算回路7に部分体元 x_1 と部分体元 y_1 とが供給され、それらの積（ $x_1 \times y_1$ ）が部分体乗算回路7により計算され、スイッチ回路22を介して記憶回路23に記憶される。

【0066】なお、このとき部分体加算回路8A、8Bには値が供給されず、記憶回路10A、10Bに記憶された値（今の場合、 $x_0 \times y_0$ ）はそのまま変化しない。

【0067】次に第3のステップ（第6のタイミング）では、スイッチ回路9Aがオン状態に制御されるとともにスイッチ回路9Bがオフ状態に制御されるとともに、スイッチ回路22が部分体乗算回路7と部分体加算回路8A、8Bとを電氣的に接続し、第1の選択回路3Aがノルム $N(\beta)$ を選択するとともに第2の選択回路6Aが記憶回路23に記憶された部分体元（ $x_1 \times y_1$ ）を選択する。したがって部分体乗算回路7にノルム $N(\beta)$ と部分体元（ $x_1 \times y_1$ ）とが供給され、それらの積（ $N(\beta) \times x_1 \times y_1$ ）が部分体乗算回路7により計算され、スイッチ回路22を介して部分体加算回路8A、8Bに供給される。

【0068】そして、部分体加算回路8A、8Bは、記憶回路10A、10Bに記憶された値（今の場合、 $x_0 \times y_0$ ）と部分体乗算回路7による積（ $N(\beta) \times x_1 \times y_1$ ）との和をそれぞれ計算する。今、スイッチ回路9Aだけがオン状態であるので、部分体加算回路8Aによる和（ $x_0 \times y_0 + N(\beta) \times x_1 \times y_1$ ）がスイッチ回路9Aを介して記憶回路10Aに記憶される。なお、記憶回路10Bには、そのまま、部分体元（ $x_0 \times y_0$ ）が保持される。

【0069】最後に第4のステップ（第7のタイミング）では、スイッチ回路9Aがオフ状態に制御されるとともにスイッチ回路9Bがオン状態に制御されるとともにスイッチ回路22が部分体乗算回路7と部分体加算回路8A、8Bとを電氣的に接続し、第1の選択回路3Aが部分体元（ $x_0 + x_1$ ）を選択するとともに第2の選択回路6Aが部分体元（ $y_0 + y_1$ ）を選択する。したがって部分体乗算回路7に部分体元（ $x_0 + x_1$ ）と部分体元（ $y_0 + y_1$ ）とが供給され、それらの積（ $(x_0 + x_1) \times (y_0 + y_1)$ ）が部分体乗算回路7により計算され、スイッチ回路22を介して部分体加算回路8A、8Bに供給される。

16

【0070】そして、部分体加算回路8Aは、記憶回路10Aに記憶された値と部分体乗算回路7による積との和を計算し、部分体加算回路8Bは、記憶回路10Bに記憶された値（今の場合、 $x_0 \times y_0$ ）と部分体乗算回路7による積（ $(x_0 + x_1) \times (y_0 + y_1)$ ）との和を計算する。今、スイッチ回路9Bだけがオン状態であるので、部分体加算回路8Bによる和（ $x_0 \times y_0 + (x_0 + x_1) \times (y_0 + y_1)$ ）がスイッチ回路9Bを介して記憶回路10Bに記憶される。なお、記憶回路10Aには、そのまま、部分体元（ $x_0 \times y_0 + N(\beta) \times x_1 \times y_1$ ）が保持される。

【0071】このようにして第1～第4のステップの処理により、元 x および元 y の積 $z (= z_0 + z_1 \times \beta)$ に対応する部分体GF（ 2^n ）の元 $z_0 (= x_0 \times y_0 + N(\beta) \times x_1 \times y_1)$ が記憶回路10Aに記憶され、また出力され、部分体GF（ 2^n ）の元 $z_1 (= x_0 \times y_0 + (x_0 + x_1) \times (y_0 + y_1))$ が記憶回路10Bに記憶され、出力される。なお、スイッチ回路9A、9B、22および第1および第2の選択回路3A、6Aの制御は、最終的に記憶回路10A、10Bに記憶される値が上述のようになれば他の方式でもよい。

【0072】以上のように、この実施の形態2によれば、 n が自然数であるガロア体GF（ 2^{2n} ）についてのガロア体乗算回路における部分体演算回路を1個の部分体乗算回路および4個の部分体加算回路としたので、その他に選択回路、スイッチ回路などが必要になるものの、全体の回路規模を低減することができるという効果が得られる。

【0073】また、演算を4つのステップに分割し、部分体演算のうち出力遅延の大きい部分体乗算を各ステップにおいて1回だけ実行するようにしたので、乗算全体での出力遅延が低減され、演算を高速に実行することができるという効果が得られる。

【0074】実施の形態3. この発明の実施の形態3によるガロア体逆元演算回路は、 n を奇数とするガロア体GF（ 2^{2n} ）の元 x の逆元 $z (= x^{-1})$ を演算するものである。図3は、この発明の実施の形態3によるガロア体逆元演算回路の構成を示すブロック図である。

【0075】図において、41Aおよび41Bは、 n を奇数とするガロア体GF（ 2^{2n} ）の部分体GF（ 2^n ）の元であってガロア体GF（ 2^{2n} ）の元 $x (= x_0 + x_1 \times \beta)$ 、 β は部分体GF（ 2^n ）に属さないガロア体GF（ 2^{2n} ）の元）に対応する部分体元 x_0 （第1の部分体元）および部分体元 x_1 （第2の部分体元）をそれぞれ供給され記憶する記憶回路であり、42は、記憶回路41Aに記憶された部分体元 x_0 および記憶回路41Bに記憶された部分体元 x_1 の和（ $x_0 + x_1$ ）を演算する第5の部分体加算回路である。

【0076】43は、記憶回路41Bに記憶された部分体元 x_1 および第5の部分体加算回路42の演算結果で

17

ある部分体元 $(x_0 + x_1)$ (第8の部分体元) のうちのいずれかを選択する第3の選択回路であり、44は、記憶回路41Aに記憶された部分体元 x_0 、記憶回路41Bに記憶された部分体元 x_1 および部分体逆元回路50による逆元のうちのいずれかを選択する第4の選択回路である。

【0077】45は、第3の選択回路43により選択された部分体元と第4の選択回路44により選択された部分体元との積を演算する部分体乗算回路であり、46は、部分体乗算回路45による積の供給先を所定のタイミ
10 ミングで切り換えるスイッチ回路である。

【0078】49は所定のタイミングでの部分体乗算回路45による積を記憶または累積し、部分体逆元回路50に供給する記憶累積回路である。記憶累積回路49において、47は、記憶回路48に記憶された部分体元と、スイッチ回路46を介して供給された部分体乗算回路45による積との和を計算する部分体加算回路であり、48は部分体加算回路47の演算結果を記憶する記憶回路である。50は、記憶回路48に記憶された部分
20 体元の逆元を演算する部分体逆元回路である。

【0079】53Aは、部分体GF(2^n)の元であってガロア体GF(2^{2n})の元xの逆元 $z (= z_0 + z_1 \times \beta)$ に対応する部分体元 z_0 (第9の部分体元)として、所定のタイミングにおいてスイッチ回路46を介して部分体乗算回路45による積を出力する第1の出力回路である。第1の出力回路53Aにおいて、51Aは、所定のタイミングにおいてオン状態になり、スイッチ回路46を介して供給される部分体乗算回路45による積を記憶回路52Aに記憶させるスイッチ回路であり、52Aは部分体元 z_0 を記憶する記憶回路である。

【0080】53Bは、逆元 $z (= z_0 + z_1 \times \beta)$ に対応する部分体元 z_1 (第10の部分体元)として、所定のタイミングにおいてスイッチ回路46を介して部分体乗算回路45による積を出力する第2の出力回路である。第2の出力回路53Bにおいて、51Bは、所定のタイミングにおいてオン状態になり、スイッチ回路46を介して供給される部分体乗算回路45による積を記憶回路52Bに記憶させるスイッチ回路であり、52Bは部分体元 z_1 を記憶する記憶回路である。

【0081】次に動作について説明する。この実施の形態3によるガロア体逆元演算回路は、 n を奇数とするガロア体GF(2^{2n})の元 $x (= x_0 + x_1 \times \beta)$ の逆元 $x^{-1} (= z = z_0 + z_1 \times \beta)$ を4ステップで計算する。
40

【0082】まず、記憶回路41A、41Bに部分体元 x_0 、 x_1 がそれぞれ供給、記憶され、記憶累積回路49の記憶回路48に初期値0が記憶される。

【0083】第1のステップ(第8のタイミング)では、スイッチ回路46が部分体乗算回路45と記憶累積回路49とを電氣的に接続し、第3の選択回路43が部
50

18

分体元 x_1 を選択するとともに第4の選択回路44が部分体元 x_1 を選択する。したがって部分体乗算回路45に部分体元 x_1 と部分体元 x_1 とが供給され、それらの積 (x_1^2) が部分体乗算回路45により計算され、スイッチ回路46を介して記憶累積回路49の部分体加算回路47に供給される。

【0084】そして、部分体加算回路47は、記憶回路48に記憶された値(今の場合、初期値0)と部分体乗算回路45による積 (x_1^2) との和を計算し、記憶回路48に記憶させる。なお、このとき、第1および第2の出力回路53A、53Bには値が供給されず特に動作しない。

【0085】次に第2のステップ(第9のタイミング)では、スイッチ回路46が部分体乗算回路45と記憶累積回路49とを電氣的に接続し、第3の選択回路43が部分体元 $(x_0 + x_1)$ を選択するとともに第4の選択回路44が部分体元 x_0 を選択する。したがって部分体乗算回路45に部分体元 $(x_0 + x_1)$ と部分体元 x_0 とが供給され、それらの積 $(x_0 \times (x_0 + x_1))$ が
20 部分体乗算回路45により計算され、スイッチ回路46を介して記憶累積回路49の部分体加算回路47に供給される。

【0086】そして、部分体加算回路47は、記憶回路48に記憶された値(今の場合、 x_1^2)と部分体乗算回路45による積 $(x_0 \times (x_0 + x_1))$ との和 $(x_1^2 + x_0 \times (x_0 + x_1))$ を計算し、記憶回路48に記憶させる。なお、このとき、第1および第2の出力回路53A、53Bには値が供給されず特に動作しない。

【0087】次に第3のステップ(第10のタイミング)では、スイッチ回路46が部分体乗算回路45と第1および第2の出力回路53A、53Bとを電氣的に接続し、第1の出力回路53Aのスイッチ回路51Aがオン状態に制御されるとともに第2の出力回路53Bのスイッチ回路51Bがオフ状態に制御され、第3の選択回路43が部分体元 $(x_0 + x_1)$ を選択するとともに、第4の選択回路44が、記憶累積回路49に累積記憶している値の部分体逆元回路50による逆元(今の場合、 $\{x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$)を選択する。

【0088】したがって部分体乗算回路45に部分体元 $(x_0 + x_1)$ と部分体元 $(\{x_1^2 + x_0 \times (x_0 + x_1)\}^{-1})$ とが供給され、それらの積 $((x_0 + x_1) \times \{x_1^2 + x_0 \times (x_0 + x_1)\}^{-1})$ が部分体乗算回路45により計算され、スイッチ回路46を介して第1および第2の出力回路53A、53Bに供給される。

【0089】そして、第1の出力回路53Aだけが、その積をスイッチ回路51Aを介して記憶回路52Aに記憶し、逆元 $x^{-1} (= z = z_0 + z_1 \times \beta)$ に対応する部分体元 $z_0 (= (x_0 + x_1) \times \{x_1^2 + x_0 \times (x_0 + x_1)\}^{-1})$ として出力する。

【0090】最後に第4のステップ(第11のタイミン

19

グ)では、スイッチ回路46が部分体乗算回路45と第1および第2の出力回路53A、53Bとを電氣的に接続し、第1の出力回路53Aのスイッチ回路51Aがオフ状態に制御されるとともに第2の出力回路53Bのスイッチ回路51Bがオン状態に制御され、第3の選択回路43が部分体元 x_1 を選択するとともに第4の選択回路44が、記憶累積回路49に累積記憶している値の部分体逆元回路50による逆元(今の場合、 $\{x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$)を選択する。

【0091】したがって部分体乗算回路45に部分体元 x_1 と部分体元 $\{x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$ とが供給され、それらの積 $(x_1 \times \{x_1^2 + x_0 \times (x_0 + x_1)\}^{-1})$ が部分体乗算回路45により計算され、スイッチ回路46を介して第1および第2の出力回路53A、53Bに供給される。

【0092】そして、第2の出力回路53Bだけが、その積をスイッチ回路51Bを介して記憶回路52Bに記憶し、逆元 $x^{-1} (= z = z_0 + z_1 \times \beta)$ に対応する部分体元 $z_1 (= x_1 \times \{x_1^2 + x_0 \times (x_0 + x_1)\}^{-1})$ として出力する。

【0093】このようにして第1～第4のステップの処理により、第1の出力回路53Aにより、元 x の逆元 $z (= z_0 + z_1 \times \beta)$ に対応する部分体GF(2^n)の元 $z_0 (= (x_0 + x_1) \times \{x_1^2 + x_0 \times (x_0 + x_1)\}^{-1})$ が記憶、出力され、第2の出力回路53Bにより、部分体GF(2^n)の元 $z_1 (= x_1 \times \{x_1^2 + x_0 \times (x_0 + x_1)\}^{-1})$ が記憶、出力される。なお、スイッチ回路46、51A、51Bおよび第3および第4の選択回路43、44の制御は、最終的に記憶回路52A、52Bに記憶される値が上述のようになれば他の方式でもよい。

【0094】以上のように、この実施の形態3によれば、 n が奇数であるガロア体GF(2^{2n})についてのガロア体逆元演算回路における部分体演算回路を1個の部分体乗算回路、2個の部分体加算回路および1個の部分体逆元回路としたので、その他に選択回路、スイッチ回路などが必要になるものの、全体の回路規模を低減することができるという効果が得られる。

【0095】また、演算を4つのステップに分割し、部分体演算のうち出力遅延の大きい部分体乗算を各ステップにおいて1回だけ実行するようにしたので、逆元演算全体での出力遅延が低減され、演算を高速に実行することができるという効果が得られる。

【0096】実施の形態4. この発明の実施の形態4によるガロア体逆元演算回路は、 n を自然数とするガロア体GF(2^{2n})の元 x の逆元 $z (= x^{-1})$ を演算するものである。図4は、この発明の実施の形態4によるガロア体逆元演算回路の構成を示すブロック図である。

【0097】図において、43Aは、記憶回路41Bに記憶された部分体元 x_1 、部分体加算回路42による和

20

である部分体元 $(x_0 + x_1)$ 、および記憶回路61に記憶されたノルム $N(\beta)$ (第11の部分体元)のうちのいずれかを選択する第3の選択回路である。

【0098】44Aは記憶回路41Aに記憶された部分体元 x_0 、記憶回路41Bに記憶された部分体元 x_1 、部分体逆元回路50による逆元、および記憶累積回路49Aの記憶回路48に記憶または累積された値のうちのいずれかを選択する第4の選択回路である。第4の選択回路44Aにおいて、63は、記憶回路41Aに記憶された部分体元 x_0 、記憶回路41Bに記憶された部分体元 x_1 、選択回路64により選択された値のうちのいずれかを選択する選択回路であり、64は、部分体逆元回路50による逆元、および記憶累積回路49Aの記憶回路48に記憶または累積された値のうちのいずれかを選択する選択回路である。

【0099】49Aは所定のタイミングでの部分体乗算回路45による積を記憶または累積し、部分体逆元回路50に供給する記憶累積回路である。記憶累積回路49Aにおいて、62は部分体加算回路47による和およびスイッチ回路46を介して供給された部分体乗算回路45による積のいずれかを選択し、選択した値を記憶回路48に記憶させる選択回路である。

【0100】61は元 x と部分体元 x_0 、 x_1 との対応関係 $(x = x_0 + x_1 \times \beta)$ を示す部分体GF(2^n)に属さないガロア体GF(2^{2n})の元 β についてのガロア体GF(2^{2n})から部分体GF(2^n)へのノルム $N(\beta)$ を供給され記憶する記憶回路である。

【0101】なお、図4におけるその他の構成要素については実施の形態3によるもの(図3)と同様であるのでその説明を省略する。また、ノルム $N(\beta)$ は図示せぬ所定の演算回路により演算され供給される。

【0102】次に動作について説明する。この実施の形態4によるガロア体逆元演算回路は、 n を自然数とするガロア体GF(2^{2n})の元 $x (= x_0 + x_1 \times \beta)$ の逆元 $x^{-1} (= z = z_0 + z_1 \times \beta)$ を5ステップで計算する。例えば n を4とすると、ガロア体GF(2^{2n})がガロア体GF(2^8)となり、その部分体GF(2^n)がガロア体GF(2^4)となる。その場合、実施の形態2と同様のガロア体GF(2^8)の基底を使用することができる。

【0103】まず、記憶回路41A、41Bに部分体元 x_0 、 x_1 がそれぞれ供給、記憶され、記憶回路61にノルム $N(\beta)$ が供給、記憶され、記憶累積回路49Aの記憶回路48に初期値0が記憶される。

【0104】第1のステップ(第12のタイミング)では、スイッチ回路46が部分体乗算回路45と記憶累積回路49Aとを電氣的に接続し、第3の選択回路43Aが部分体元 x_1 を選択するとともに第4の選択回路44Aが部分体元 x_1 を選択し、選択回路62は、部分体乗算回路45による積を選択する。したがって部分体乗算

21

回路 4 5 に部分体元 x_1 と部分体元 x_1 とが供給され、それらの積 (x_1^2) が部分体乗算回路 4 5 により計算され、スイッチ回路 4 6 を介して記憶累積回路 4 9 A の部分体加算回路 4 7 および選択回路 6 2 に供給される。

【0105】そして、部分体加算回路 4 7 は記憶回路 4 8 に記憶された値と部分体乗算回路 4 5 による積との和を計算して選択回路 6 2 に供給するが、今の場合、選択回路 6 2 は部分体乗算回路 4 5 による積 (x_1^2) を選択し、記憶回路 4 8 に記憶させる。なお、このとき、第 1 および第 2 の出力回路 5 3 A, 5 3 B には値が供給されず特に動作しない。

【0106】次に第 2 のステップ (第 13 のタイミング) では、スイッチ回路 4 6 が部分体乗算回路 4 5 と記憶累積回路 4 9 A とを電氣的に接続し、第 3 の選択回路 4 3 A がノルム $N(\beta)$ を選択するとともに第 4 の選択回路 4 4 A が記憶回路 4 8 に記憶された部分体元 (今の場合、 x_1^2) を選択し、選択回路 6 2 は、部分体乗算回路 4 5 による積を選択する。したがって部分体乗算回路 4 5 にノルム $N(\beta)$ と部分体元 (x_1^2) とが供給され、それらの積 ($N(\beta) \times x_1^2$) が部分体乗算回路 4 5 により計算され、スイッチ回路 4 6 を介して記憶累積回路 4 9 A の部分体加算回路 4 7 および選択回路 6 2 に供給される。

【0107】そして、部分体加算回路 4 7 は、記憶回路 4 8 に記憶された値と部分体乗算回路 4 5 による積との和を計算して選択回路 6 2 に供給するが、今の場合、選択回路 6 2 は部分体乗算回路 4 5 による積 ($N(\beta) \times x_1^2$) を選択し、記憶回路 4 8 に記憶させる。なお、このとき、第 1 および第 2 の出力回路 5 3 A, 5 3 B には値が供給されず特に動作しない。

【0108】次に第 3 のステップ (第 14 のタイミング) では、スイッチ回路 4 6 が部分体乗算回路 4 5 と記憶累積回路 4 9 A とを電氣的に接続し、第 3 の選択回路 4 3 A が部分体元 ($x_0 + x_1$) を選択するとともに第 4 の選択回路 4 4 A が部分体元 x_0 を選択し、選択回路 6 2 は、部分体加算回路 4 7 による和を選択する。したがって部分体乗算回路 4 5 に部分体元 ($x_0 + x_1$) と部分体元 x_0 とが供給され、それらの積 ($(x_0 + x_1) \times x_0$) が部分体乗算回路 4 5 により計算され、スイッチ回路 4 6 を介して記憶累積回路 4 9 A の部分体加算回路 4 7 および選択回路 6 2 に供給される。

【0109】そして、部分体加算回路 4 7 は記憶回路 4 8 に記憶された値 (今の場合、 $N(\beta) \times x_1^2$) と部分体乗算回路 4 5 による積 ($x_0 \times (x_0 + x_1)$) との和を計算して選択回路 6 2 に供給し、選択回路 6 2 は、部分体加算回路 4 7 による和 ($N(\beta) \times x_1^2 + x_0 \times (x_0 + x_1)$) を選択し、記憶回路 4 8 に記憶させる。なお、このとき、第 1 および第 2 の出力回路 5 3 A, 5 3 B には値が供給されず特に動作しない。

【0110】次に第 4 のステップ (第 15 のタイミン

22

グ) では、スイッチ回路 4 6 が部分体乗算回路 4 5 と第 1 および第 2 の出力回路 5 3 A, 5 3 B とを電氣的に接続し、第 1 の出力回路 5 3 A のスイッチ回路 5 1 A がオン状態に制御されるとともに第 2 の出力回路 5 3 B のスイッチ回路 5 1 B がオフ状態に制御され、第 3 の選択回路 4 3 A が部分体元 ($x_0 + x_1$) を選択するとともに第 4 の選択回路 4 4 A が部分体逆元回路 5 0 による逆元 (今の場合、 $\{N(\beta) \times x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$) を選択する。

【0111】したがって部分体乗算回路 4 5 に部分体元 ($x_0 + x_1$) と部分体元 ($\{N(\beta) \times x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$) とが供給され、それらの積 ($(x_0 + x_1) \times \{N(\beta) \times x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$) が部分体乗算回路 4 5 により計算され、スイッチ回路 4 6 を介して第 1 および第 2 の出力回路 5 3 A, 5 3 B に供給される。

【0112】そして、第 1 の出力回路 5 3 A だけが、その積をスイッチ回路 5 1 A を介して記憶回路 5 2 A に記憶し、逆元 x^{-1} ($= z = z_0 + z_1 \times \beta$) に対応する部分体元 z_0 ($= (x_0 + x_1) \times \{N(\beta) \times x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$) として出力する。

【0113】最後に第 5 のステップ (第 16 のタイミング) では、スイッチ回路 4 6 が部分体乗算回路 4 5 と第 1 および第 2 の出力回路 5 3 A, 5 3 B とを電氣的に接続し、第 1 の出力回路 5 3 A のスイッチ回路 5 1 A がオフ状態に制御されるとともに第 2 の出力回路 5 3 B のスイッチ回路 5 1 B がオン状態に制御され、第 3 の選択回路 4 3 A が部分体元 x_1 を選択するとともに第 4 の選択回路 4 4 A が、部分体逆元回路 5 0 による逆元 (今の場合、 $\{N(\beta) \times x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$) を選択する。

【0114】したがって部分体乗算回路 4 5 に部分体元 x_1 と部分体元 ($\{N(\beta) \times x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$) とが供給され、それらの積 ($x_1 \times \{N(\beta) \times x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$) が部分体乗算回路 4 5 により計算され、スイッチ回路 4 6 を介して第 1 および第 2 の出力回路 5 3 A, 5 3 B に供給される。

【0115】そして、第 2 の出力回路 5 3 B だけが、その積をスイッチ回路 5 1 B を介して記憶回路 5 2 B に記憶し、逆元 x^{-1} ($= z = z_0 + z_1 \times \beta$) に対応する部分体元 z_1 ($= x_1 \times \{N(\beta) \times x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$) として出力する。

【0116】このようにして第 1 ~ 第 5 のステップの処理により、第 1 の出力回路 5 3 A により、元 x の逆元 z ($= z_0 + z_1 \times \beta$) に対応する部分体 GF (2^n) の元 z_0 ($= (x_0 + x_1) \times \{N(\beta) \times x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$) が記憶、出力され、第 2 の出力回路 5 3 B により、部分体 GF (2^n) の元 z_1 ($= x_1 \times \{N(\beta) \times x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$) が記

23

憶、出力される。なお、スイッチ回路 46、51A、51B および第 3 および第 4 の選択回路 43A、44A の制御は、最終的に記憶回路 52A、52B に記憶される値が上述のようになれば他の方式でもよい。

【0117】 以上のように、この実施の形態 4 によれば、 n が自然数であるガロア体 $GF(2^{2n})$ についてのガロア体逆元演算回路における部分体演算回路を 1 個の部分体乗算回路、2 個の部分体加算回路および 1 個の部分体逆元回路としたので、その他に選択回路、スイッチ回路などが必要になるものの、全体の回路規模を低減することができるといふ効果が得られる。

【0118】 また、演算を 5 つのステップに分割し、部分体演算のうち出力遅延の大きい部分体乗算を各ステップにおいて 1 回だけ実行するようにしたので、逆元演算全体での出力遅延が低減され、演算を高速に実行することができるという効果が得られる。

【0119】

【発明の効果】 以上のように、この発明によれば、ガロア体 $GF(2^{2n})$ (n は奇数) の部分体 $GF(2^n)$ の元であってガロア体 $GF(2^{2n})$ の第 1 の元に対応する第 1 の部分体元および第 2 の部分体元の和を第 3 の部分体元として演算する第 1 の部分体加算回路と、部分体の元であってガロア体 $GF(2^{2n})$ の第 2 の元に対応する第 4 の部分体元と第 5 の部分体元との和を第 6 の部分体元として演算する第 2 の部分体加算回路と、第 1 の部分体元、第 2 の部分体元および第 3 の部分体元のうちのいずれかを選択する第 1 の選択回路と、第 4 の部分体元、第 5 の部分体元および第 6 の部分体元のうちのいずれかを選択する第 2 の選択回路と、第 1 の選択回路により選択された部分体元と第 2 の選択回路により選択された部分体元との積を演算する部分体乗算回路と、第 1 の元および第 2 の元の積に対応する部分体の 2 つの元のうちの一方となる部分体の元を記憶する第 1 の記憶回路と、第 1 の元および第 2 の元の積に対応する部分体の 2 つの元のうちの他方となる部分体の元を記憶する第 2 の記憶回路と、第 1 の記憶回路に記憶された部分体の元と部分体乗算回路による積との和を演算する第 3 の部分体加算回路と、第 2 の記憶回路に記憶された部分体の元と部分体乗算回路による積との和を演算する第 4 の部分体加算回路と、所定のタイミングにおいて第 3 の部分体加算回路による和で第 1 の記憶回路に記憶された部分体の元を更新する第 1 の更新回路と、所定のタイミングにおいて第 4 の部分体加算回路による和で第 2 の記憶回路に記憶された部分体の元を更新する第 2 の更新回路とで構成するようにしたので、全体の回路規模を低減することができるという効果がある。

【0120】 この発明によれば、第 1 の記憶回路および第 2 の記憶回路に初期値として 0 が記憶され、第 1 のタイミングで、第 1 の選択回路が第 1 の部分体元を選択するとともに第 2 の選択回路が第 4 の部分体元を選択し、

24

第 1 および第 2 の更新回路が更新をし、第 2 のタイミングで、第 1 の選択回路が第 2 の部分体元を選択するとともに第 2 の選択回路が第 5 の部分体元を選択し、第 1 の更新回路が更新をし、第 3 のタイミングで、第 1 の選択回路が第 3 の部分体元を選択するとともに第 2 の選択回路が第 6 の部分体元を選択し、第 2 の更新回路が更新するようにしたので、乗算全体での出力遅延が低減され、演算を高速に実行することができるという効果がある。

【0121】 この発明によれば、 n を自然数とするガロア体 $GF(2^{2n})$ について、第 1 の選択回路が第 1 の部分体元、第 2 の部分体元、第 3 の部分体元、およびガロア体 $GF(2^{2n})$ から部分体 $GF(2^n)$ へのノルムである第 7 の部分体元のうちのいずれかを選択し、第 2 の選択回路が第 4 の部分体元、第 5 の部分体元、第 6 の部分体元、および部分体乗算回路による積のうちのいずれかを選択するようにしたので、全体の回路規模を低減することができるという効果がある。

【0122】 この発明によれば、第 1 の記憶回路および第 2 の記憶回路に初期値として 0 が記憶され、第 4 のタイミングで、第 1 の選択回路が第 1 の部分体元を選択するとともに第 2 の選択回路が第 4 の部分体元を選択し、第 1 の更新および第 2 の更新回路が更新をし、第 5 のタイミングで、第 1 の選択回路が第 2 の部分体元を選択し、第 2 の選択回路が第 5 の部分体元を選択した後に第 6 のタイミングで、第 1 の選択回路が第 7 の部分体元を選択するとともに第 2 の選択回路が第 5 のタイミングにおける部分体乗算回路による積を選択し、第 1 の更新回路が更新をし、第 7 のタイミングで、第 1 の選択回路が第 3 の部分体元を選択するとともに第 2 の選択回路が第 6 の部分体元を選択し、第 2 の更新回路が更新をするようにしたので、乗算全体での出力遅延が低減され、演算を高速に実行することができるという効果がある。

【0123】 この発明によれば、ガロア体 $GF(2^{2n})$ (n は奇数) の部分体 $GF(2^n)$ の元であってガロア体 $GF(2^{2n})$ の元に対応する第 1 の部分体元および第 2 の部分体元の和を第 8 の部分体元として演算する第 5 の部分体加算回路と、第 2 の部分体元および第 8 の部分体元のうちのいずれかを選択する第 3 の選択回路と、部分体 $GF(2^n)$ の元の逆元を演算する部分体逆元回路と、第 1 の部分体元、第 2 の部分体元、および部分体逆元回路による逆元のうちのいずれかを選択する第 4 の選択回路と、第 3 の選択回路により選択された部分体元と第 4 の選択回路により選択された部分体元との積を演算する部分体乗算回路と、所定のタイミングでの部分体乗算回路による積を記憶または累積し、部分体逆元回路に供給する記憶累積回路と、部分体 $GF(2^n)$ の元であってガロア体 $GF(2^{2n})$ の元の逆元に対応する第 9 の部分体元および第 10 の部分体元のうちの第 9 の部分体元として所定のタイミングにおいて部分体乗算回路による積を出力する第 1 の出力回路と、第 10 の部分体元と

25

して所定のタイミングにおいて部分体乗算回路による積を出力する第2の出力回路とで構成するようにしたので、全体の回路規模を低減することができるという効果がある。

【0124】この発明によれば、第8のタイミングで、第3の選択回路が第2の部分体元を選択するとともに第4の選択回路が第2の部分体元を選択し、記憶累積回路が部分体乗算回路による積を記憶し、第9のタイミングで、第3の選択回路が第8の部分体元を選択するとともに第4の選択回路が第1の部分体元を選択し、記憶累積回路が記憶している値を部分体逆元回路に供給した後に部分体乗算回路による積を累積記憶し、第10のタイミングで、第3の選択回路が第8の部分体元を選択するとともに第4の選択回路が部分体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第1の出力回路が出力をし、第11のタイミングで、第3の選択回路が第2の部分体元を選択するとともに第4の選択回路が部分体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第2の出力回路が出力をするようにしたので、逆元演算全体での出力遅延が低減され、演算を高速に実行することができるという効果がある。

【0125】この発明によれば、 n を自然数とするガロア体 $GF(2^{2n})$ について、第3の選択回路が第2の部分体元、第8の部分体元、およびガロア体 $GF(2^{2n})$ から部分体 $GF(2^n)$ へのノルムである第11の部分体元のうちのいずれかを選択し、第4の選択回路が第1の部分体元、第2の部分体元、部分体逆元回路による逆元、および記憶累積回路に記憶または累積された値のうちのいずれかを選択するようにしたので、全体の回路規模を低減することができるという効果がある。

【0126】この発明によれば、第12のタイミングで、第3の選択回路が第2の部分体元を選択するとともに第4の選択回路が第2の部分体元を選択し、記憶累積回路が部分体乗算回路による積を記憶し、第13のタイミングで、第3の選択回路が第11の部分体元を選択するとともに第4の選択回路が記憶累積回路の記憶値を選択し、記憶累積回路が記憶している値を第4の選択回路に供給した後に部分体乗算回路による積を記憶し、第1

26

4のタイミングで、第3の選択回路が第8の部分体元を選択するとともに第4の選択回路が第1の部分体元を選択し、記憶累積回路が部分体乗算回路による積を累積記憶し、第15のタイミングで、第3の選択回路が第8の部分体元を選択するとともに第4の選択回路が部分体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第1の出力回路が出力をし、第16のタイミングで、第3の選択回路が第2の部分体元を選択するとともに第4の選択回路が部分体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第2の出力回路が出力をするようにしたので、逆元演算全体での出力遅延が低減され、演算を高速に実行することができるという効果がある。

【図面の簡単な説明】

【図1】 この発明の実施の形態1によるガロア体乗算回路の構成を示すブロック図である。

【図2】 この発明の実施の形態2によるガロア体乗算回路の構成を示すブロック図である。

【図3】 この発明の実施の形態3によるガロア体逆元演算回路の構成を示すブロック図である。

【図4】 この発明の実施の形態4によるガロア体逆元演算回路の構成を示すブロック図である。

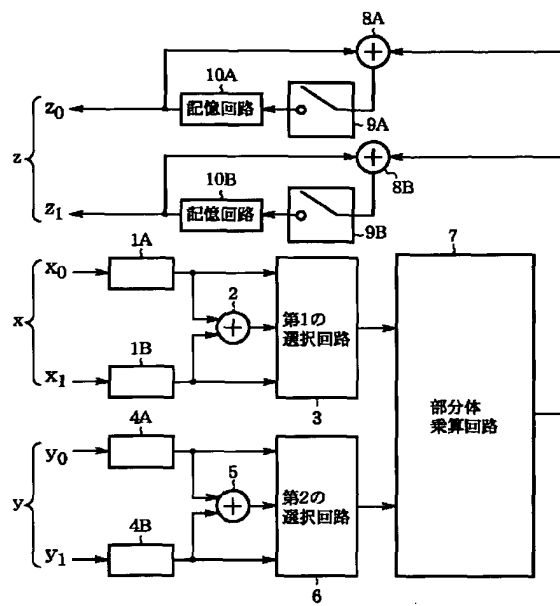
【図5】 従来のガロア体乗算回路を示すブロック図である。

【図6】 従来のガロア体逆元演算回路を示すブロック図である。

【符号の説明】

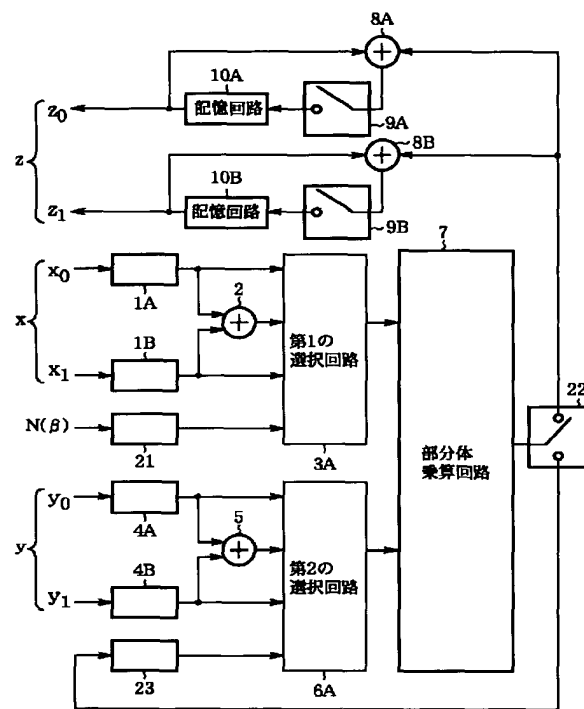
2 第1の部分体加算回路、3、3A 第1の選択回路、5 第2の部分体加算回路、6、6A 第2の選択回路、7 部分体乗算回路、8A 第3の部分体加算回路、8B 第4の部分体加算回路、9A スイッチ回路（第1の更新回路）、9B スイッチ回路（第2の更新回路）、10A 記憶回路（第1の記憶回路）、10B 記憶回路（第2の記憶回路）、42 第5の部分体加算回路、43、43A 第3の選択回路、44、44A 第4の選択回路、45 部分体乗算回路、50 部分体逆元回路、53A 第1の出力回路、53B 第2の出力回路。

【図1】



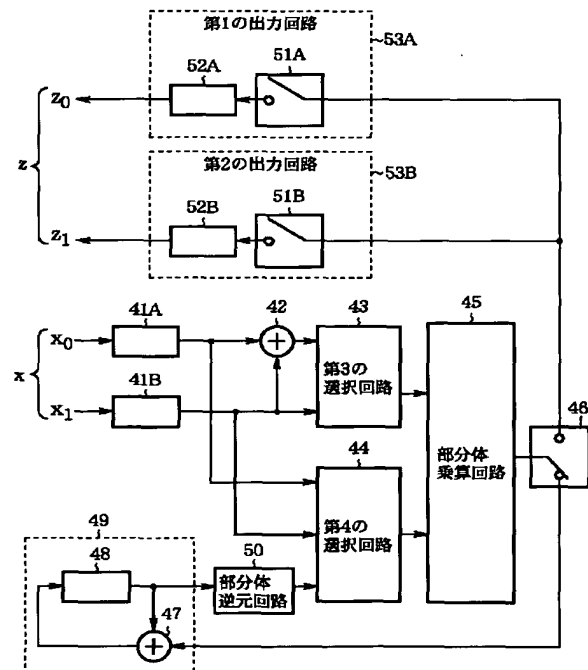
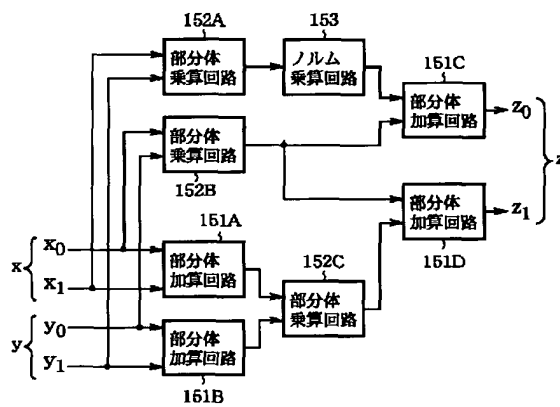
2: 第1の部分体加算回路
 5: 第2の部分体加算回路
 8A: 第3の部分体加算回路
 8B: 第4の部分体加算回路
 9A: スイッチ回路 (第1の更新回路)
 9B: スイッチ回路 (第2の更新回路)
 10A: 記憶回路 (第1の記憶回路)
 10B: 記憶回路 (第2の記憶回路)

【図2】



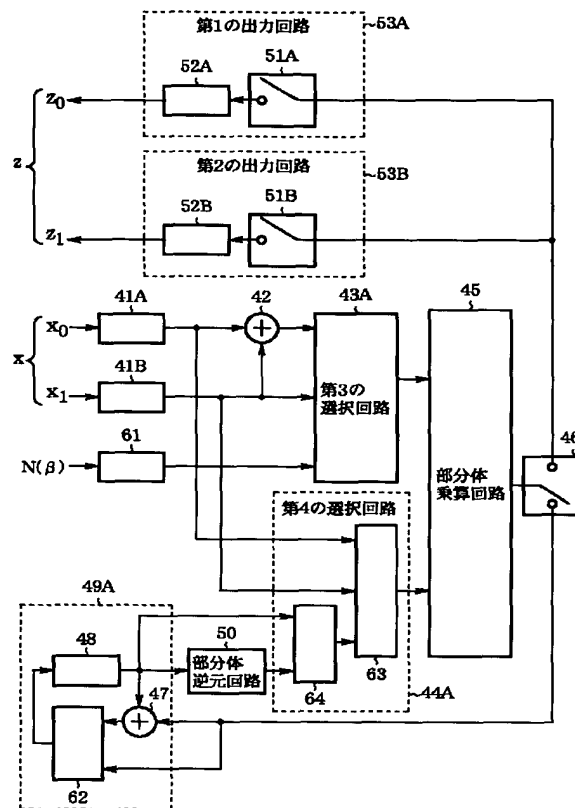
【図3】

【図5】



42: 第5の部分体加算回路

【図4】



【図6】

